FORTINET

Adaptívne zabezpečenie pre SOC tímy

Orchestrácia, Automatizácia a Reakcia

15 Million

Botnet C&C attempts

TWHARTED

PER MINUTE

© Fortinet Inc. All Rights Reserved.

462,217

Malicious Website

URL

ACCESSES Blocked Per Minute

© Fortinet Inc. All Rights Reserved.

5.3 Million

NETWORK INTRUSION ATTEMPTS

resisted per minute

© Fortinet Inc. All Rights Reserved.

136,173 PHISHING

BLOCKED PER MINUTE

© Fortinet Inc. All Rights Reserved.

903,860

MALWARE PROGRAMS

Neutralized Per Minute

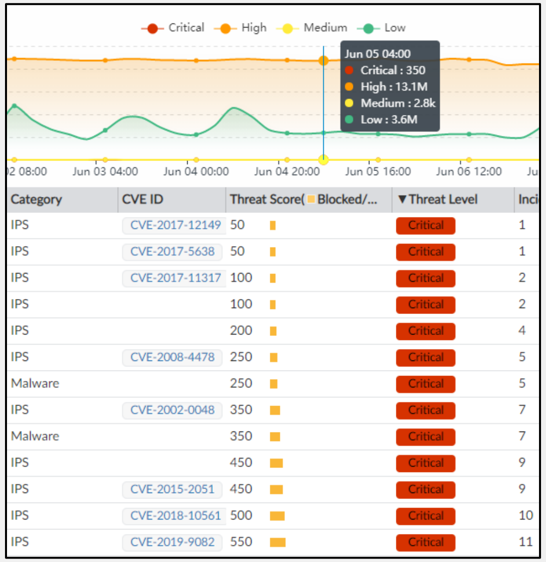
© Fortinet Inc. All Rights Reserved.

EVENTS per DAY?

31,395,240,000

© Fortinet Inc. All Rights Reserved.

SOC Challenges



Category	CVE ID	Threat Score(Blocked/...	▼Threat Level	Inci
IPS	CVE-2017-12149	50	Critical	1
IPS	CVE-2017-5638	50	Critical	1
IPS	CVE-2017-11317	100	Critical	2
IPS		100	Critical	2
IPS		200	Critical	4
IPS	CVE-2008-4478	250	Critical	5
Malware		250	Critical	5
IPS	CVE-2002-0048	350	Critical	7
Malware		350	Critical	7
IPS		450	Critical	9
IPS	CVE-2015-2051	450	Critical	9
IPS	CVE-2018-10561	500	Critical	10
IPS	CVE-2019-9082	550	Critical	11

Alert Overload

- Lot of detection technologies
- Huge volume of data

Disparate Tools

- Multiple consoles like SIEMs, Threat Intels, EDRs, Sandboxes …
- Limited integration

Manual Processes

- Poor documentation
- Analysts do not follow processes
- Tribal knowledge

Talent Shortage

- global cybersecurity workforce gap
  1.8 million by 2022

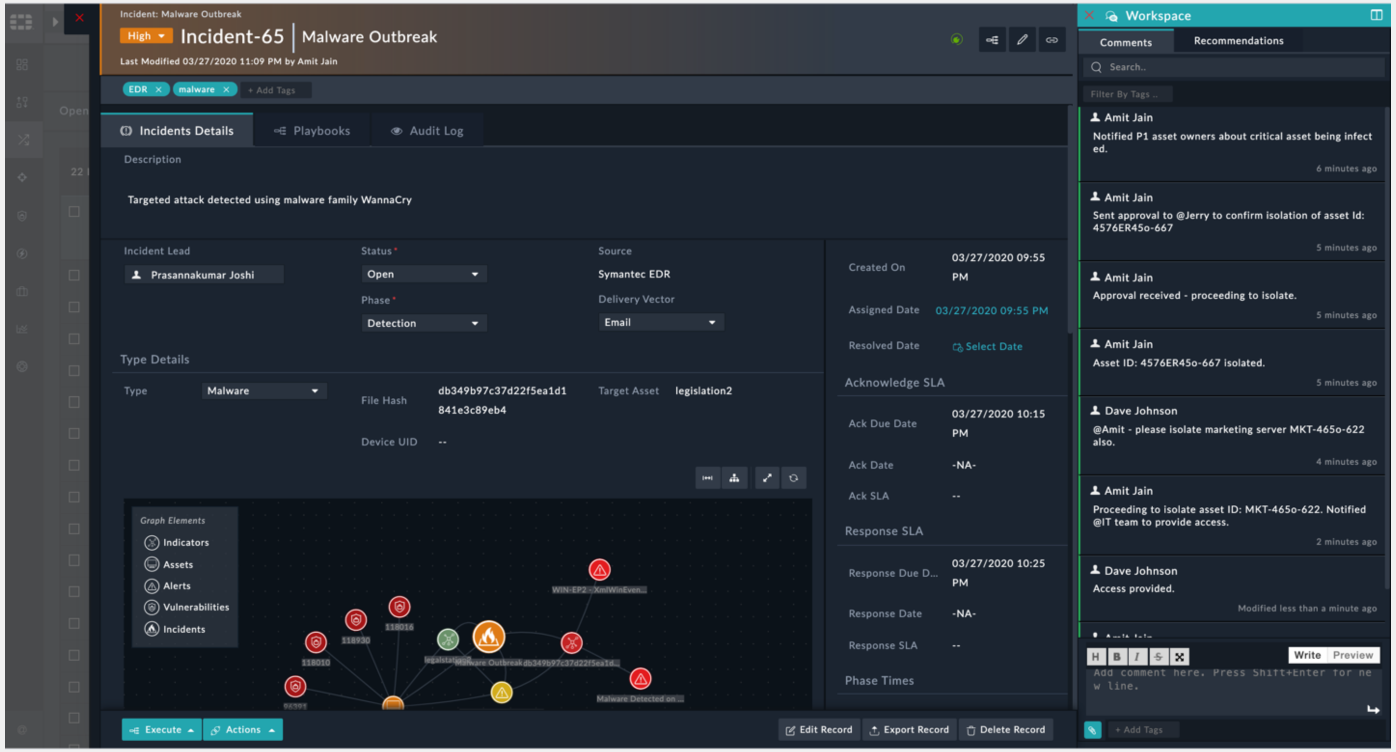
© Fortinet Inc. All Rights Reserved.

AI-driven Security Operations

FortiSOAR: Incident Response Component - Alerts & Incidents

A single place to view & organize security data to reduce the manual effort of going to disparate security tools

- Track entire incident life cycle
  - details, status, assigned human, last updated date/time
- Record Linking
  - link assets, users, Indicators and vulnerabilities
- Intuitive and customizable view
  - List/Grid view, filter & search
- Ticket system integration



Incident: Malware Outbreak

High Incident-65 | Malware Outbreak

Last Modified 03/27/2020 11:09 PM by Amit Jain

Description

Targeted attack detected using malware family WannaCry

Incident Lead: Prasannakumar Joshi

Status: Open

Phase: Detection

Source: Symantec EDR

Delivery Vector: Email

Type Details

Type: Malware

File Hash: db349b97c37d22f5ea1d1841e3c89eb4

Device UID: --

Target Asset: legislation2

Created On: 03/27/2020 09:55 PM

Assigned Date: 03/27/2020 09:55 PM

Resolved Date: Select Date

Acknowledge SLA

Ack Due Date: 03/27/2020 10:15 PM

Ack Date: -NA-

Ack SLA: --

Response SLA

Response Due D...: 03/27/2020 10:25 PM

Response Date: -NA-

Response SLA: --

Phase Times

Amit Jain: Notified P1 asset owners about critical asset being infected. — 6 minutes ago

Amit Jain: Sent approval to @Jerry to confirm isolation of asset Id: 4576ER45o-667 — 5 minutes ago

Amit Jain: Approval received - proceeding to isolate. — 5 minutes ago

Amit Jain: Asset ID: 4576ER45o-667 isolated. — 5 minutes ago

Dave Johnson: @Amit - please isolate marketing server MKT-465o-622 also. — 4 minutes ago

Amit Jain: Proceeding to isolate asset ID: MKT-465o-622. Notified @IT team to provide access. — 2 minutes ago

Dave Johnson: Access provided. — Modified less than a minute ago

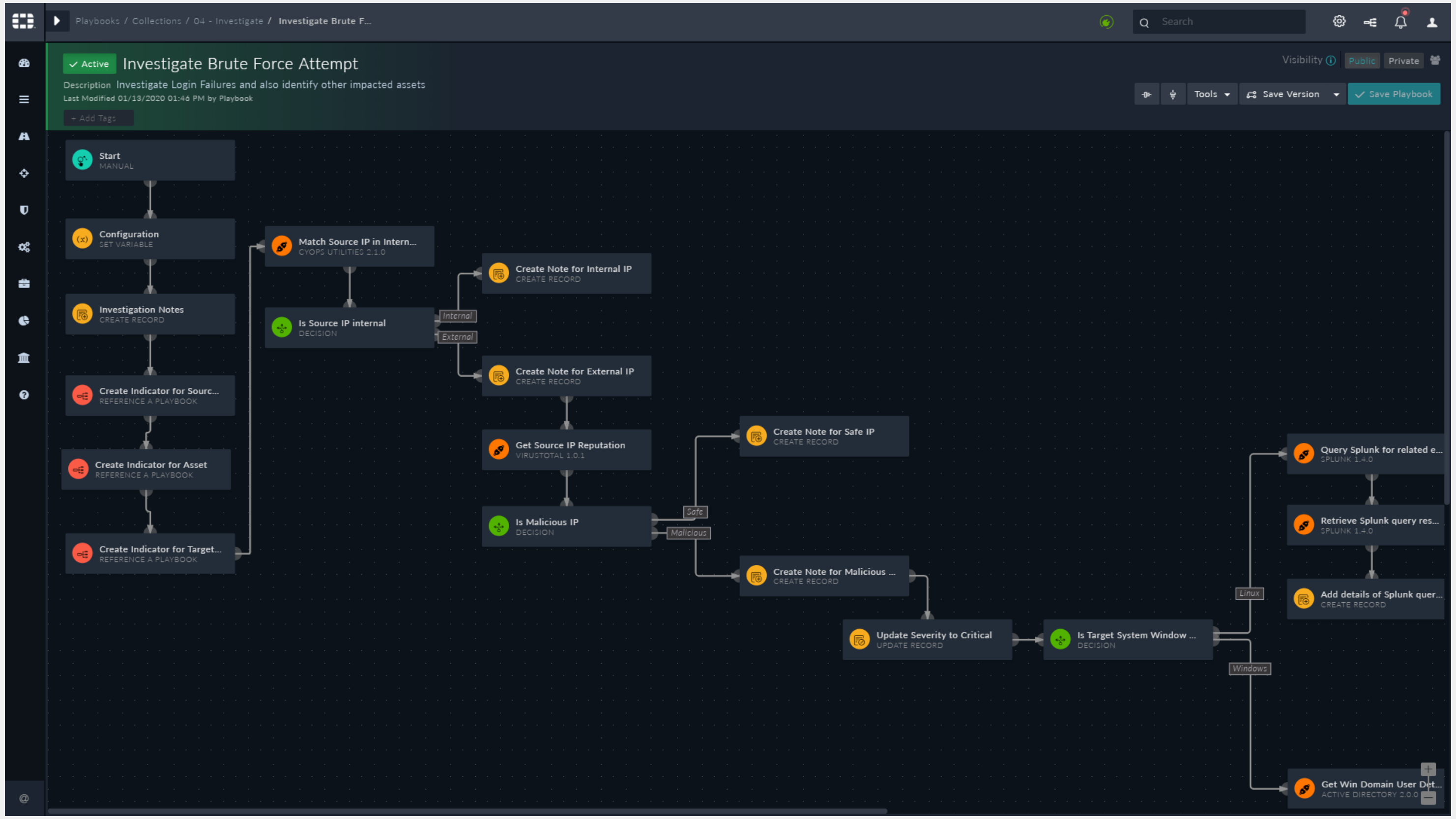
© Fortinet Inc. All Rights Reserved.

AI-driven Security Operations

FortiSOAR: Orchestration and Automation with playbooks

Build your best practices and entire workflow into the playbooks for consistent Incident handling and response

- Drag and drop to modify or add a step to a playbook
- Variety of selection choices from graphical menus
  - Create/Update/Find records
  - Logical decisions, approvals and tasks
  - Connectors and utilities
  - Nested playbooks



Playbooks / Collections / 04 - Investigate / Investigate Brute F...

✓ Active Investigate Brute Force Attempt

Description Investigate Login Failures and also identify other impacted assets

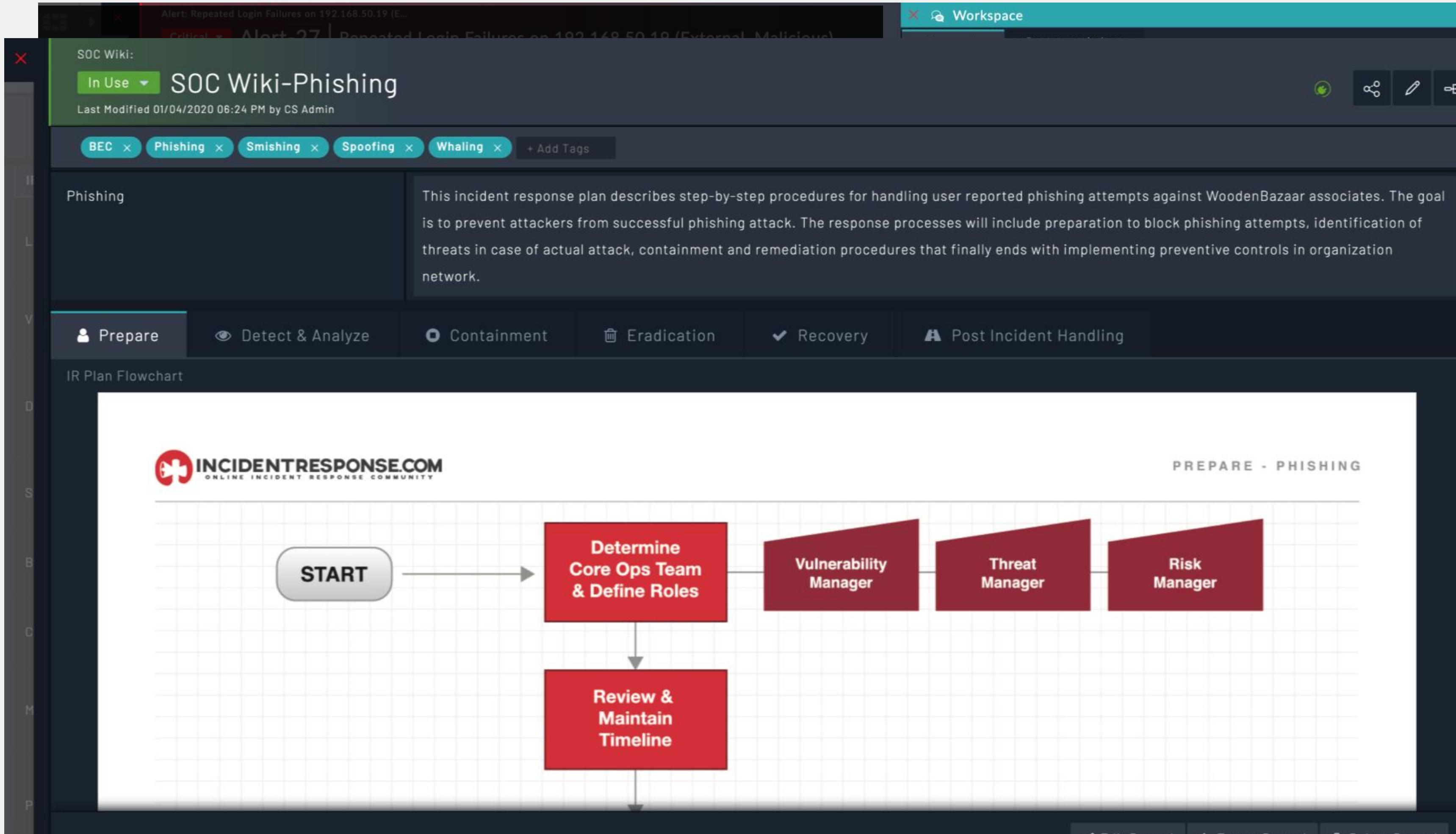
Last Modified 01/13/2020 01:46 PM by Playbook

AI-driven Security Operations

FortiSOAR: Workspace collaboration & Knowledge Sharing

Each incident or alert has a workspace pane with a built-in ‘chat’ channel for SOC analysts to collaborate and perform actions

- Workspace Comment Panel
- Use Knowledge Sharing Component to create SOC Wiki for knowledge sharing and team collaboration



Alert: Repeated Login Failures on 192.168.50.19 (E...

Workspace

SOC Wiki:

In Use SOC Wiki-Phishing

Last Modified 01/04/2020 06:24 PM by CS Admin

BEC × Phishing × Smishing × Spoofing × Whaling × + Add Tags

Phishing

This incident response plan describes step-by-step procedures for handling user reported phishing attempts against WoodenBazaar associates. The goal is to prevent attackers from successful phishing attack. The response processes will include preparation to block phishing attempts, identification of threats in case of actual attack, containment and remediation procedures that finally ends with implementing preventive controls in organization network.

Prepare | Detect & Analyze | Containment | Eradication | Recovery | Post Incident Handling

IR Plan Flowchart

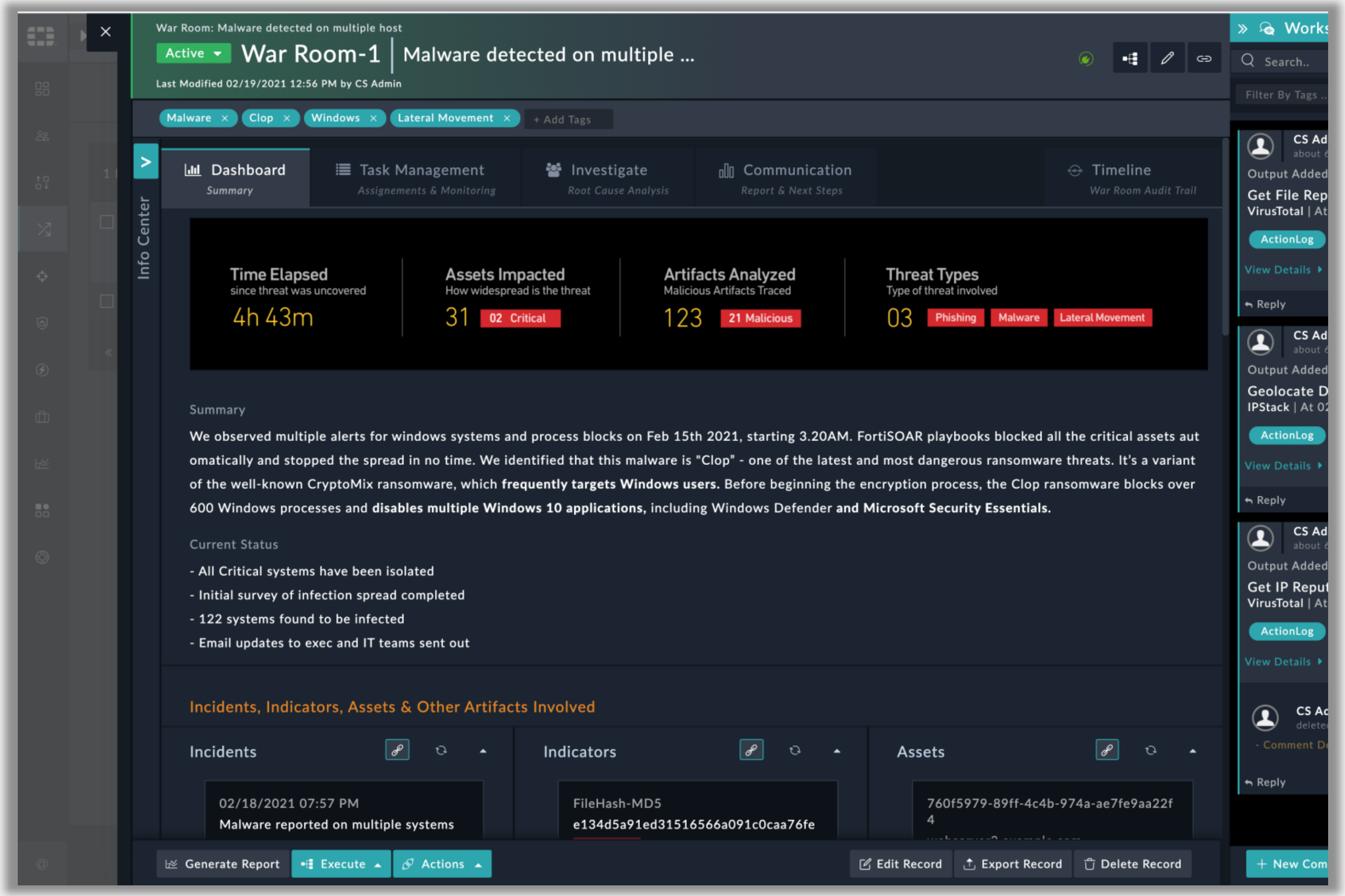
INCIDENTRESPONSE.COM
ONLINE INCIDENT RESPONSE COMMUNITY
PREPARE - PHISHING
START
Determine Core Ops Team & Define Roles
Vulnerability Manager
Threat Manager
Risk Manager
Review & Maintain Timeline

AI-driven Security Operations

FortiSOAR: Incident War Room

Advanced crisis management and real-time team collaboration, built around four pillars –*Communicate, Coordinate, Investigate, Escalate*

- Internal information gathering
- Internal communication & visibility to executives and employees
- Shared situational awareness across teams
- Built-in task management, investigation arena, collaboration, reporting, announcements and much more for streamlining P1 investigations



War Room: Malware detected on multiple host

Active War Room-1 | Malware detected on multiple ...

Last Modified 02/19/2021 12:56 PM by CS Admin

Time Elapsed
since threat was uncovered
4h 43m

Assets Impacted
How widespread is the threat
31 02 Critical

Artifacts Analyzed
Malicious Artifacts Traced
123 21 Malicious

Threat Types
Type of threat involved
03 Phishing Malware Lateral Movement

Summary

We observed multiple alerts for windows systems and process blocks on Feb 15th 2021, starting 3.20AM. FortiSOAR playbooks blocked all the critical assets automatically and stopped the spread in no time. We identified that this malware is "Clop" - one of the latest and most dangerous ransomware threats. It's a variant of the well-known CryptoMix ransomware, which **frequently targets Windows users.** Before beginning the encryption process, the Clop ransomware blocks over 600 Windows processes and **disables multiple Windows 10 applications,** including Windows Defender **and Microsoft Security Essentials.**

Current Status

- All Critical systems have been isolated
- Initial survey of infection spread completed
- 122 systems found to be infected
- Email updates to exec and IT teams sent out

Incidents, Indicators, Assets & Other Artifacts Involved

Incidents
02/18/2021 07:57 PM
Malware reported on multiple systems

Indicators
FileHash-MD5
e134d5a91ed31516566a091c0caa76fe

Assets
760f5979-89ff-4c4b-974a-ae7fe9aa22f
4

CS Ad
about
Output Added
Get File Rep
VirusTotal | At

CS Ad
about
Output Added
Geolocate D
IPStack | At 02

CS Ad
about
Output Added
Get IP Reput
VirusTotal | At

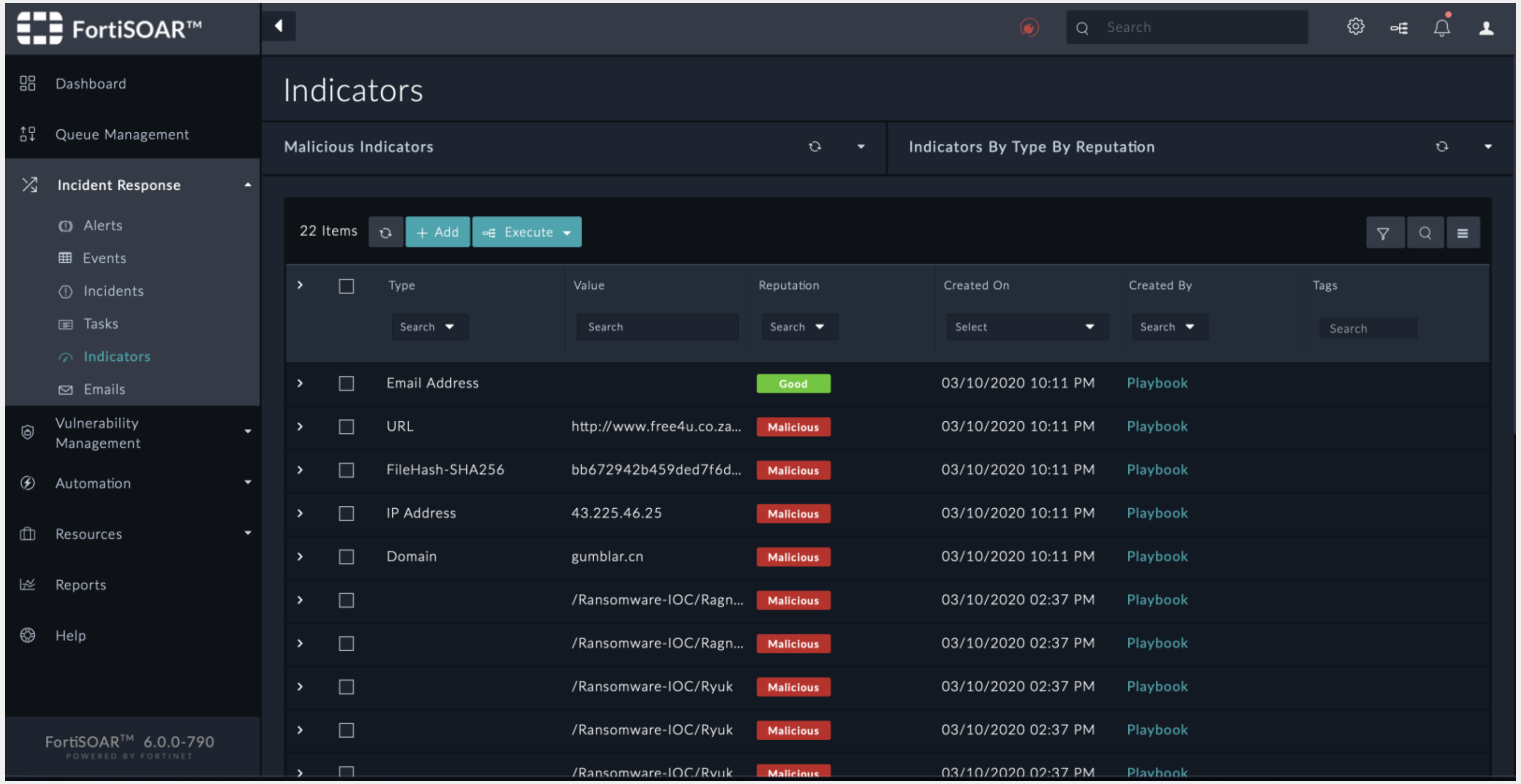
CS Ac
delete
- Comment D

AI-driven Security Operations

FortiSOAR: Threat Intel Management – Indicators

Managing multiple TI formats and sources from a central location and link the threat data to alerts and incidents

- Extracts threat intel from alert data, uploaded files, emails, and external threat intelligence sources
- Store the threat info in the DB for other modules to use



Indicators

Malicious Indicators

Indicators By Type By Reputation

22 Items

	☐	Type	Value	Reputation	Created On	Created By	Tags
		Search	Search	Search	Select	Search	Search
›	☐	Email Address		Good	03/10/2020 10:11 PM	Playbook	
›	☐	URL	http://www.free4u.co.za...	Malicious	03/10/2020 10:11 PM	Playbook	
›	☐	FileHash-SHA256	bb672942b459ded7f6d...	Malicious	03/10/2020 10:11 PM	Playbook	
›	☐	IP Address	43.225.46.25	Malicious	03/10/2020 10:11 PM	Playbook	
›	☐	Domain	gumblar.cn	Malicious	03/10/2020 10:11 PM	Playbook	
›	☐		/Ransomware-IOC/Ragn...	Malicious	03/10/2020 02:37 PM	Playbook	
›	☐		/Ransomware-IOC/Ragn...	Malicious	03/10/2020 02:37 PM	Playbook	
›	☐		/Ransomware-IOC/Ryuk	Malicious	03/10/2020 02:37 PM	Playbook	
›	☐		/Ransomware-IOC/Ryuk	Malicious	03/10/2020 02:37 PM	Playbook	
›	☐		/Ransomware-IOC/Ryuk	Malicious	03/10/2020 02:37 PM	Playbook	

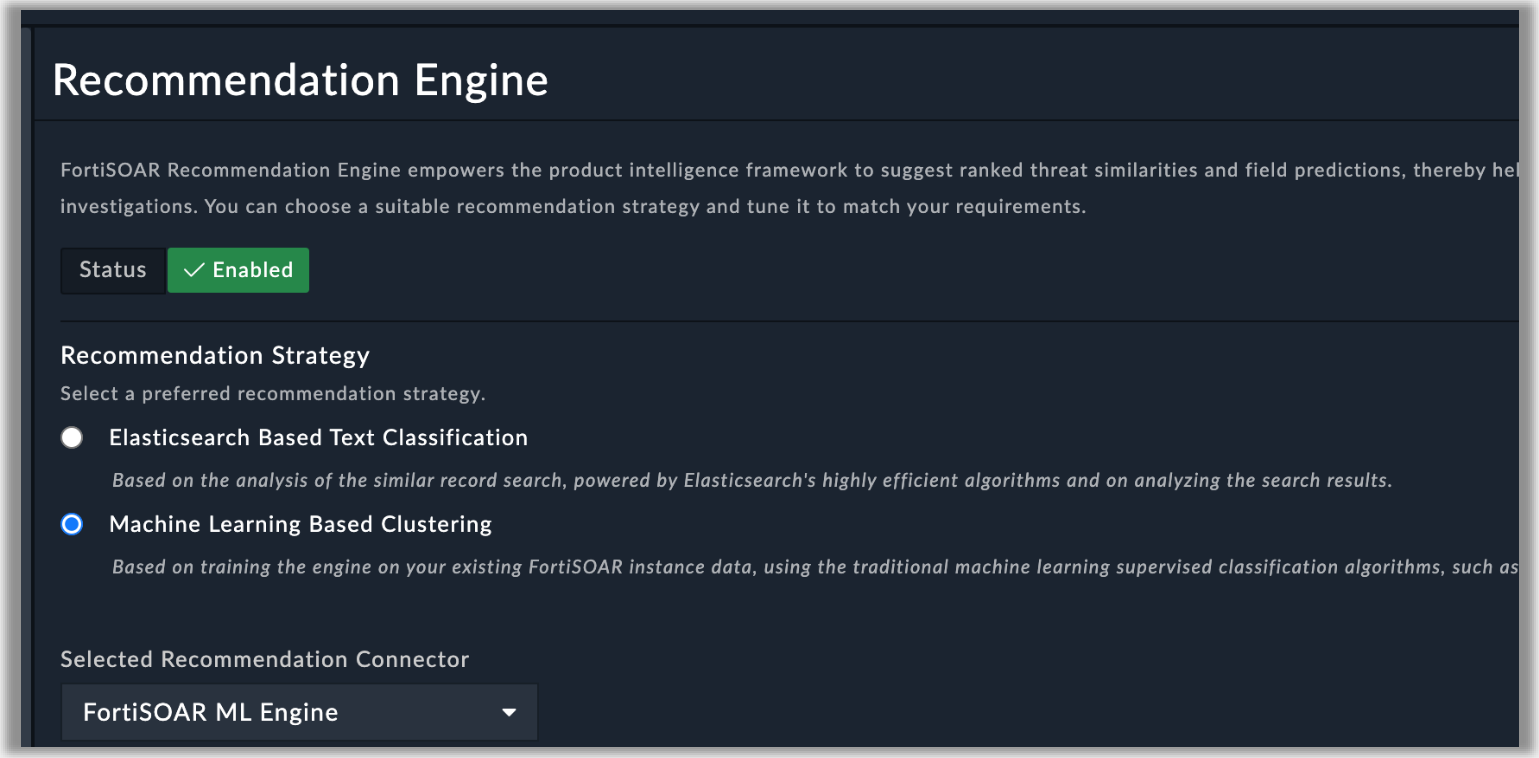
© Fortinet Inc. All Rights Reserved.

AI-driven Security Operations

FortiSOAR: ML-Powered Recommendation Engine

Machine-learning based clustering strategy added to the FSR Recommendation Engine, making it more powerful and dynamic

- Allows to choose desired ML model
- Users can decide training frequency
- Users can specify on what parameters will the model be trained and for what kind of predictions it will be used
- Users can leverage the results for similar threats, field predictions and auto-population of fields during ingestion



Recommendation Engine

FortiSOAR Recommendation Engine empowers the product intelligence framework to suggest ranked threat similarities and field predictions, thereby hel investigations. You can choose a suitable recommendation strategy and tune it to match your requirements.

Status ✓ Enabled

Recommendation Strategy

Select a preferred recommendation strategy.

○ Elasticsearch Based Text Classification

Based on the analysis of the similar record search, powered by Elasticsearch's highly efficient algorithms and on analyzing the search results.

● Machine Learning Based Clustering

Based on training the engine on your existing FortiSOAR instance data, using the traditional machine learning supervised classification algorithms, such as

Selected Recommendation Connector

FortiSOAR ML Engine

© Fortinet Inc. All Rights Reserved.

Benefits of SOAR solution

Analyst Productivity (3-10 times)

Faster Response Time To Alerts (80% faster)

Reduce Volume Of Alers

© Fortinet Inc. All Rights Reserved.

FORTINET®